AFRL-IF-RS-TR-2006-357
Final Technical Report
December 2006

INFORMATION OPERATIONS INNOVATION NETWORK (IOIN) DEMONSTRATION

Northrop Grumman Information Technology & ITT Industries

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

NOTICE AND SIGNATURE PAGE

AFRL-IF-RS-TR-2006-357 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/

BRIAN T. SPINK
Work Unit Manager

/s/

WARREN H. DEBANY Jr.
Technical Advisor, Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE	*Form Approved* **OMB No. 0704-0188**

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
DEC 2006	Final	Oct 05 – Sep 06

4. TITLE AND SUBTITLE	
INFORMATION OPERATIONS INNOVATION NETWORK (IOIN) DEMONSTRATION	5a. CONTRACT NUMBER FA8750-05-D-0260/0002
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER 28021F
6. AUTHOR(S) Vic Choo and Louis Scheiderich	5d. PROJECT NUMBER CIAC
	5e. TASK NUMBER QG
	5f. WORK UNIT NUMBER 02
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Northrop Grumman Information Technology & ITT Industries 525 Brooks Rd Rome NY 13441-4505	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFRL/IFGA 525 Brooks Rd Rome NY 13441-4505	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSORING/MONITORING AGENCY REPORT NUMBER AFRL-IF-RS-TR-2006-357

12. DISTRIBUTION AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# 06-818

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The NetD COP/Situational Awareness effort demonstrates the application of AFRL technology to providing enhanced situational awareness and visualization techniques for network defense. In particular, the program illustrates the following key points: Provide an operational view of the network security information; Move from intrusion detection to attack detection; Relate the impact of network defense to the larger mission; and Supplement existing/future network defense tools with additional capabilities. The actual software packages used for this effort include VIAasst, VisAlert, Flexviewer, Event Correlation for Cyber Attack Recognition (ECCARS) and the SQL Correlator. The results of the effort show that the system is capable of providing and enhanced situational awareness on live network discs.

15. SUBJECT TERMS

Situational Awareness (SA), Measure of Effectiveness (MOE), Data Extraction Utility (DEU), Event Correlation for Cyber Attack Recognition (ECCARS)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Brian Spink
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (*Include area code)*
U	U	U	UL	23	

Table of Contents

List of Figures

1.0 Introduction

Northrop Grumman was tasked to demonstrate a Network Defense Common Operational Picture (NetD COP) and Network Situational Awareness (SA) capability to operational users in support of the Information Operations Innovation Network (IOIN) evaluation funded by the Air Combat Command (ACC). The purpose of the demonstration was to show the operational communities technology that can be operationally ready within the next 12 months. This also provides the operational community with a chance to provide feedback to the Air Force Labs regarding their needs, preferences, and requirements.

The scope of this effort is limited to designing, implementing, and conducting an evaluation of NetD COP and SA systems, as they apply to current network defense operations systems. The demonstration was to integrate the developed visualization and situational awareness software and systems into the existing computer network defense systems in order to address deficiencies and operational usefulness issues. Minor changes to the existing software were required in order to accomplish this task.

In this paper, NetD COP primarily refers to visualization methods while SA refers to data collection and correlation. This paper provides a high level overview of the NetD COP and SA experiments.

2.0 Background

Current network defense capabilities are manpower intensive and do not fully promote the sharing of information required to provide a high degree of situational awareness and analysis capabilities to network defense personnel. The Air Force Research Laboratory (AFRL) has been performing research on visualization, correlation, and data interfacing methods for network security data over the past several years. As a result, AFRL proposed the demonstration of these capabilities as part of a Network Defense Common Operational Picture (NetD COP) and Situational Awareness (SA) experiments for the Information Operations Innovation Network (IOIN). The objectives of the experiments are:

- Provide an operational view of the network security information
- Move from intrusion detection to attack detection
- Relate the impact of network defense to the larger mission
- Supplement existing/future network defense tools with additional capabilities

The approach of this effort included integrating a Net-D COP capability based on the FlexViewer Security Management System (FSMS) with a situational awareness module. The FSMS consists of a number of components including: Mission Definition, Status Monitoring, Incident Management, IT Risk Status, External System Interfaces, and Administrative functions that provide the following capabilities:

- Enhanced Information Assurance visualization
- Provisions to allow Joint and Coalition forces to share, access and retrieve data
- Mission impact analysis for critical assets
- Ability to detect intrusion, disruptions of services and threats to AF networks.
- Ability to determine network weak points, mission impacts and system degradation.
- Real-time response to internal and external network suspicious activity for both wired and wireless communication networks.
- Integrated capability to monitor and display AF information systems.

The situational awareness module performs the following additional functions:

- Analyzes and transform network intrusion detection data into actionable events.
- Identifies C2 impact by correlating IP's attacked to mission function.
-

This integrated suite or NetD COP system was then installed at a single operational site selected by the customer. This report describes the demonstration scenario or experiments, the capabilities provided, lessons learned and the evaluation results.

3.0 Demonstration

As previously stated, the NetD COP/Situational Awareness demonstration has four primary goals. These goals seek to provide commanders and analysts with better awareness of the network security status and its potential impacts. This ability is achieved by merging existing sensor data (e.g., information sources) together with emerging correlation/fusions and visualization tools. The visualization tools present the information to the user in an effective and efficient manner.

The architecture for the NetD COP/Situational Awareness demonstration is illustrated in **Error! Reference source not found.**.

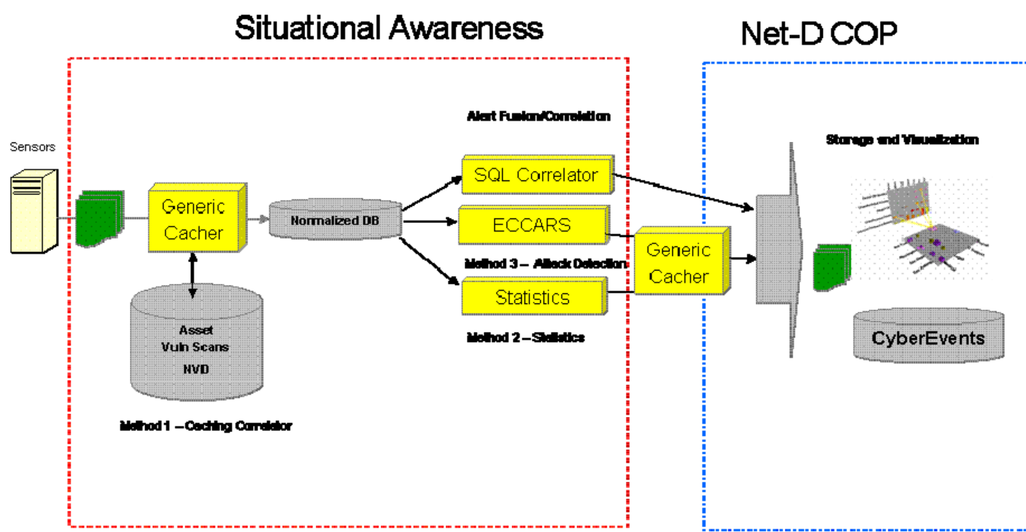

Figure 1. NetD COP/Situational Awareness Block Diagram

The correlation/fusion tools analyze the sensor data in order to reduce the number of alerts by identifying sequences of information that indicate that a potential attack is occurring. The tools combine events (e.g., sensor output) into correlated Cyber Alerts.

The hardware implementation of the demonstration system is illustrated in Figure 2.

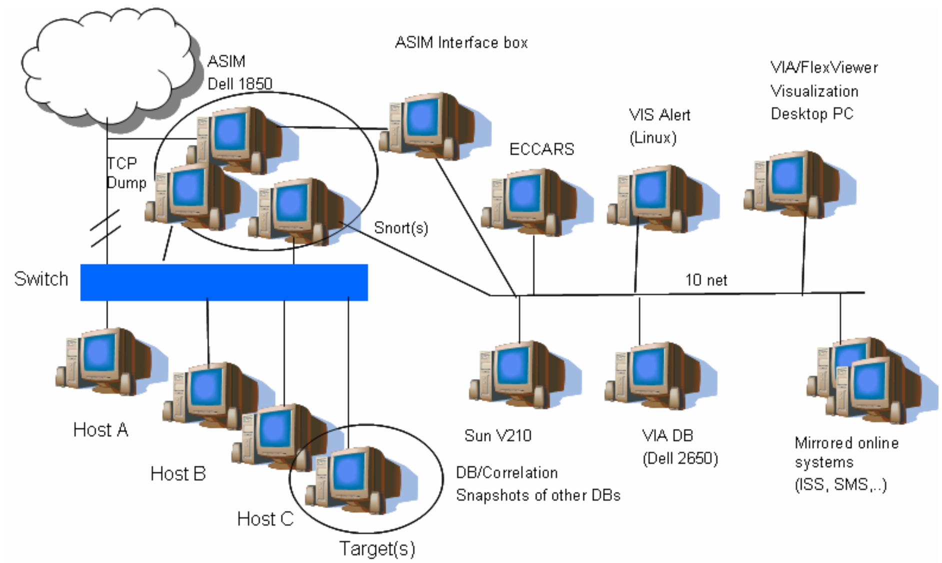

Figure 2. IOIN Demonstration Hardware Configuration

This allows analysts to focus their efforts on those particular areas. A description of each of these components is described is provided next.

3.1 Sensors

The term sensor is interpreted to generically represent all input data sources. The sensors include intrusion detection systems but as well as data sources such as network management systems and other network security tools. For this effort, a focus was placed on using sensors that already exist at ACC. The sensors used to support this demonstration include the following:

- Automated Security Incident Management (ASIM) – An ASIM Intrusion Detection sensor was provided by AFIWC to support this experiment. The ASIM sensor was placed inside the ACC network and reported information to an ASIM Interface box which in turn, reported data to the IOIN server database system.

- Snort – A freeware Intrusion Detection sensor was installed on a system that was also connected inside the ACC network at an alternate location.

- TCP Dump – A freeware application used to collect packet data collected data on a portion of the ACC network.

- Microsoft Systems Management Server (SMS) – A data dump from SMS was provided by ACC.

- Internet Security Scanner (ISS) – A partial vulnerability scan was provided by ACC.

A few sensors, mainly Snort and TCP Dump, were employed to capture additional data due our ability to freely configure these tools.

3.2 Infrastructure

There are a number of infrastructure components that are critical to the system.

3.2.1 IOIN Server

The IOIN Server is the central data repository of the system. This is an Oracle database that stores the majority of the information that is used by the system.

3.2.2 Data Extraction Utility (DEU)

The Data Extraction Utility is a powerful application that is used to transfer data from one database or log file to another. In this application, we use the DEU to transfer data from the ASIM Interface box and Snort sensors to the IOIN Server. The DEU also transfers data from the IOIN Server to the VIAssist system.

The DEU consists of a tap (server) and bridge (client). The tap resides on the sensor systems and retrieves data from the ASIM and Snort databases, parses/filters the information, encrypts the data, allows the bridges to connect and retrieve the information. The bridges which reside on the IOIN Server, pulls the information, un-encrypts the data, and stores it in the IOIN Server database. The DEU contains all the functions to securely transfer the information in a fast and efficient manner. Both the tap and bridge have XML formatted configuration files which tells them where to obtain the data, how to parse/filter it, who is allowed to receive the data, and where to place it and how to format it. The tap and bridge also have a number of built in features to ensure reliable operation including heart beats (timed communications to acknowledge that all components are functioning), bookmarking (identifies what data has been sent and stored to prevent duplicate data from being sent), automatic restart (all components automatically restart if the network connection or system is shutdown), and throttling (data rates are controlled to prevent receiving systems from being flooded with data).

3.3 Situational Awareness (SA)

The SA portion of the demonstration focuses on the correlation of the network security data and asset information. The SA component is designed to collect data from various sensors and perform correlation in order to identify attack indictors. The specific correlation goals of the SA engine are: 1) reduce the number of overall alerts; 2) provide positive attack indications; and 3) relate events to missions. These objectives are achieved using a series of different correlation approaches.

The SA receives sensor data from intrusion detection sensors, log files, vulnerability scanners, mission data, and asset information. The sensor information is transferred to the main processing system using one or more Data Extraction Utilities (DEU). The DEU is a client/server application that parses the sensor data and transmits it to the main data base (e.g., IOIN Server). The various correlation and fusion tools acquire the information from the IOIN Server, perform the analysis, and report important results back to the IOIN Server as “cyber alerts”. The following describes a few of the correlation methods employed.

3.3.1 Caching Correlator

The first level of correlation occurs in the transfer of data from the sensor to the IOIN Server Database. The Caching Correlator, an AFRL developed tool, uses a modified version of the DEU. This correlator allows the DEU to perform a series of data checks and add metadata to an alert before it is stored in the database. The Caching Correlator performs this function by storing specified lookup tables in memory and performing a fast check of the incoming data.

This technique supports the implementation of decision trees such as the one shown in Figure 3.

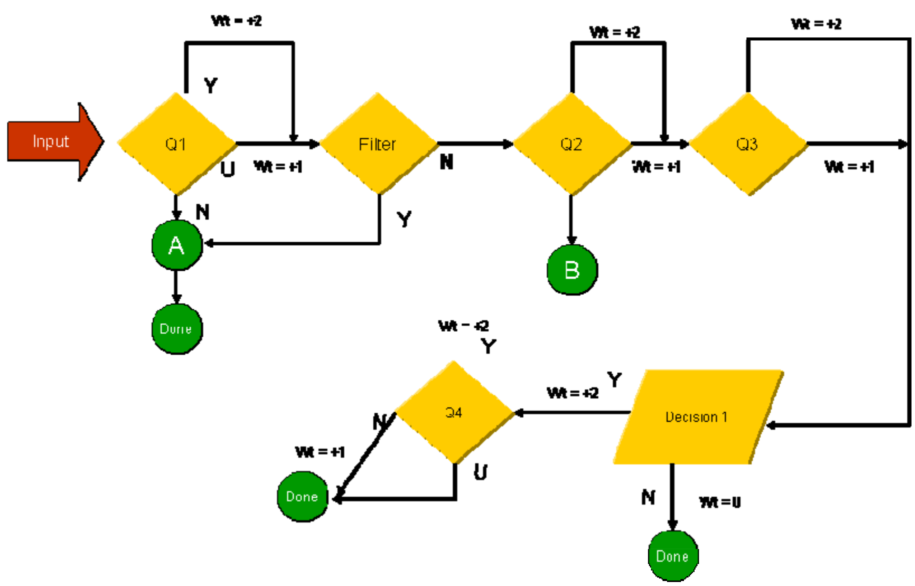

Figure 3. Generic Decision Tree

The input represents a data object structure that may correspond to an intrusion detection system event or a collection of events. The input data object traverses the decision tree. The tree contains a series of questions, denoted Q1, Q2…, that need to be answered. A weighting function is applied to the data object based upon the answers to the questions. At the end of a tree, a composite weighting function is computed in order to calculate the relative importance of the input object.

3.3.2 SQL Correlator

The SQL Correlator is a utility that is programmed to implement data correlation via SQL queries to a database. These methods apply grouping methods to aggregate events based on parameters such as total alerts, signature type, source IPs, source IP country of origin, mission of victim system, on- to-many and many-to-one relationships. This correlator is primarily intended to implement the queries developed by analysts using the Flexviewer, described later in this Technical Report. The conditions that are identified are tagged and written back to the IOIN Server's Cyber Alert table as items of interest.

3.3.3 Event Correlation for Cyber Attack Recognition (ECCARS)

The third correlation method uses a tool called the Event Correlation for Cyber Attack Recognition (ECCARS). ECCARS is a system made up of an information fusion engine and several supporting functions as illustrated in Figure 4. The fusion engine uses a modified graph matching technique for correlating alerts and mapping the alerts in such a way as to identify attack sequences. This approach monitors network events from many different network sensors in near real-time and composes the events into actions or attack tracks matching pre-determined general and/or specific cyber attack models or attack steps. As attacks are evolving, ECCARS presents a prioritized list of possible attack tracks within a network and enables an analyst to drill down into the supporting data comprising the attack track.

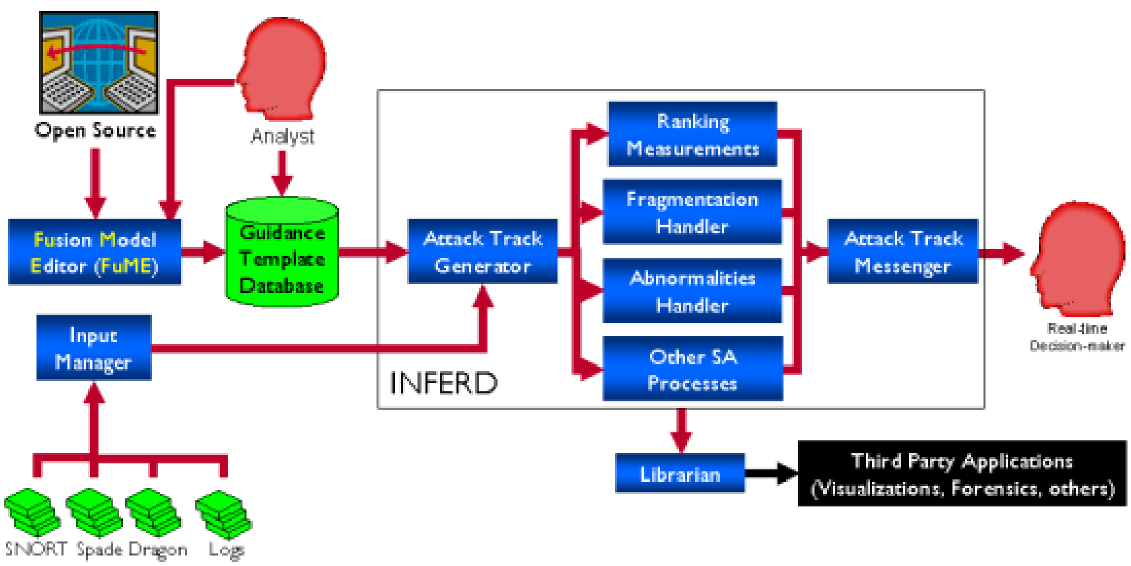

Figure 4. ECCARS Architecture

The outputs of all three correlation methods are stored in a common database for visualization using the NetD COP components.

3.4 Visualization

The NetD COP, or visualization component of demonstration focuses more on visualization techniques to provide an enhanced situational awareness to the user. The tools used for this demonstration were developed by several organizations and contractors. These tools include the AFRL FlexViewer, Secure Decision's Visualization for Information Assurance (VIA) Assist, Secure Decisions' Secure Scope, and the University of Utah's VisAlert program. The latter is being provided as a demonstration capability and is not officially part of the demonstration system. The visualization tools provide complimentary capabilities that range from spreadsheet formats to graphical awareness displays.

The NetD COP can be used in several different modes. The appropriate technique depends on how the individual user prefers to view their data. The first mode uses the FlexViewer to identify areas of potential interest based upon data aggregation. Here, the user identifies how to group the data (e.g., by source IP (SRCIP), destination IP (DESTIP), signature, number of occurrences, etc.)

An analyst workstation was created for this demonstration. It consists of two PC's that drive five different displays. A keyboard/video/mouse (KVM) switch allows one person to manipulate all the displays. The analyst workstation is show in Figure 5.

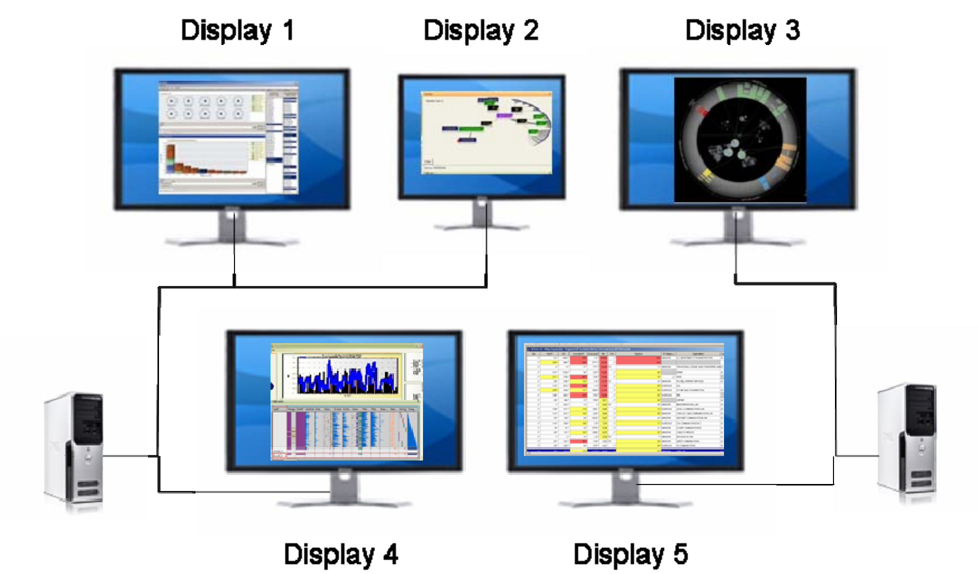

Figure 5. IOIN Analyst Workstation

Displays 1, 2, and 4 are linked to one computer while Displays 3 and 5 are linked to a second display. The intent is the top row (e.g., Displays 1, 2, and 3) will provide high level indications of problem areas. The second row (e.g., Displays 4 and 5) are used by the analyst to investigate alerts. The analyst may drag views from the top row to one of the bottom displays in order to view the data in greater detail. The planned contents of each display are described below:

- Display 1 provides a VIAssist “dashboard” view that shows charts of the Top 10 events in selected categories such as Source IP, Destination IP, Ports,…

- Display 2 provides a VIAssist “Star Tree” view that shows relationships between Source IP’s, Destination IP’s, Signatures, Severity, and Missions.

- Display 3 provides a real time display of VisAlert that shows signatures and Source IP’s mapping to hosts.

- Display 4 shows the VisAlert Table Lens, a Parabox, and other displays which the analyst activity uses to explore relationships between the sensor data.

- Display 5 displays the FlexViewer which provides near real-time indications of suspicious activity.

The following sections describe the visualization tools in more detail.

3.4.1 Flexviewer

The Flexviewer is an extensible, highly-configurable data visualization and manipulation environment that provides the analyst with a high degree of control over data presentation, and extensive analytical tools. The tool has an XML configuration file that the user can specify the locations of the data sources to utilize, what data to acquire, and how to parse and display the information The user can also specify color codes and filtering routines to create user defined views. The application allows the use to display multiple data sets at one time. One unique feature is that the application allows the user to specify data drill downs which may include executing additional queries or passing data to and launching third party applications.

A sample screenshot of the Flexviewer application is show in Figure 6.

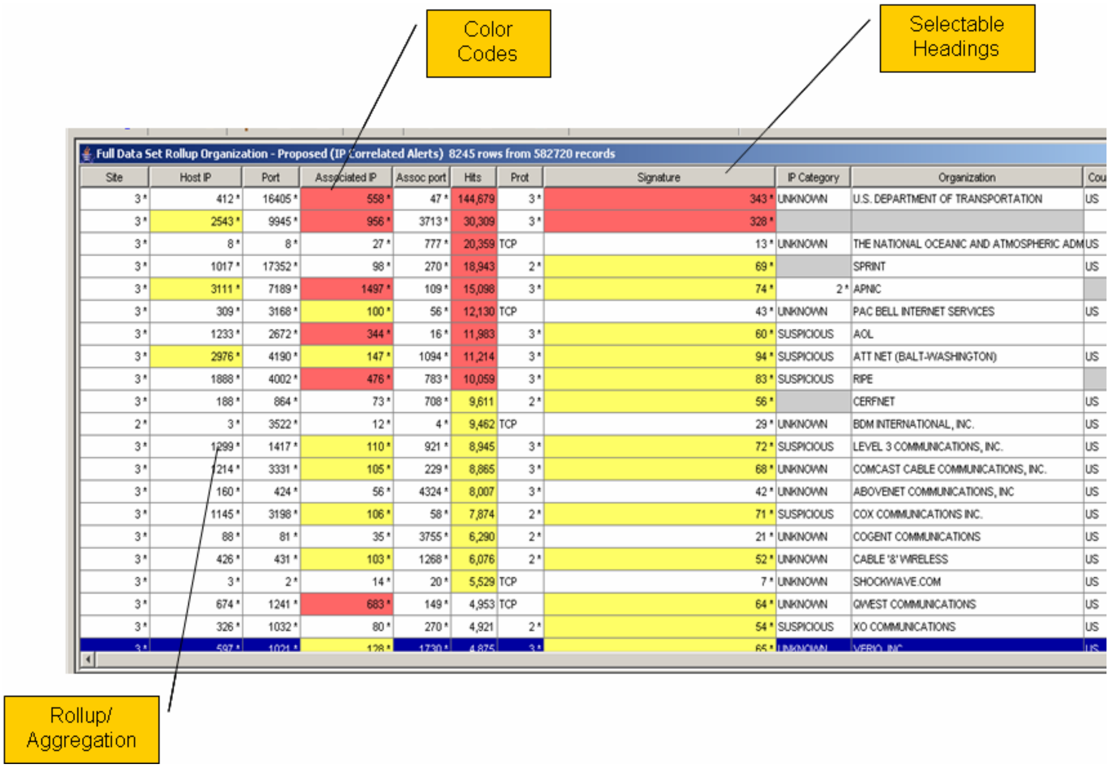

Figure 6. Flexviewer Screenshot

In the demonstration, the Flexviewer will highlight a number of data relationships in near real-time. The relationships, including one-to-many and many-to-one event mappings, will be displayed using a series of color codes to illustrate problem areas.

3.4.2 VIAssist

VIAssist is a tool developed by Secure Decisions under Government contract. VIAssist is a visualization integration platform that combines several tools (e.g., Advizor, InXight, DotNetCharting). VIAssist combines various graphing, charting, and data discovery views to that allow analysts to identify relationships between data. VIAssist links the integrated tools together such that data highlighted in one display automatically highlights all the relevant data in the other views (e.g., a coordinated view).

VIAssist has its own Sybase database which is loaded with the data of interest. The user can select which views to display and the parameters to load into each display. Some of the relevant displays for this effort are illustrated in Figure 7.

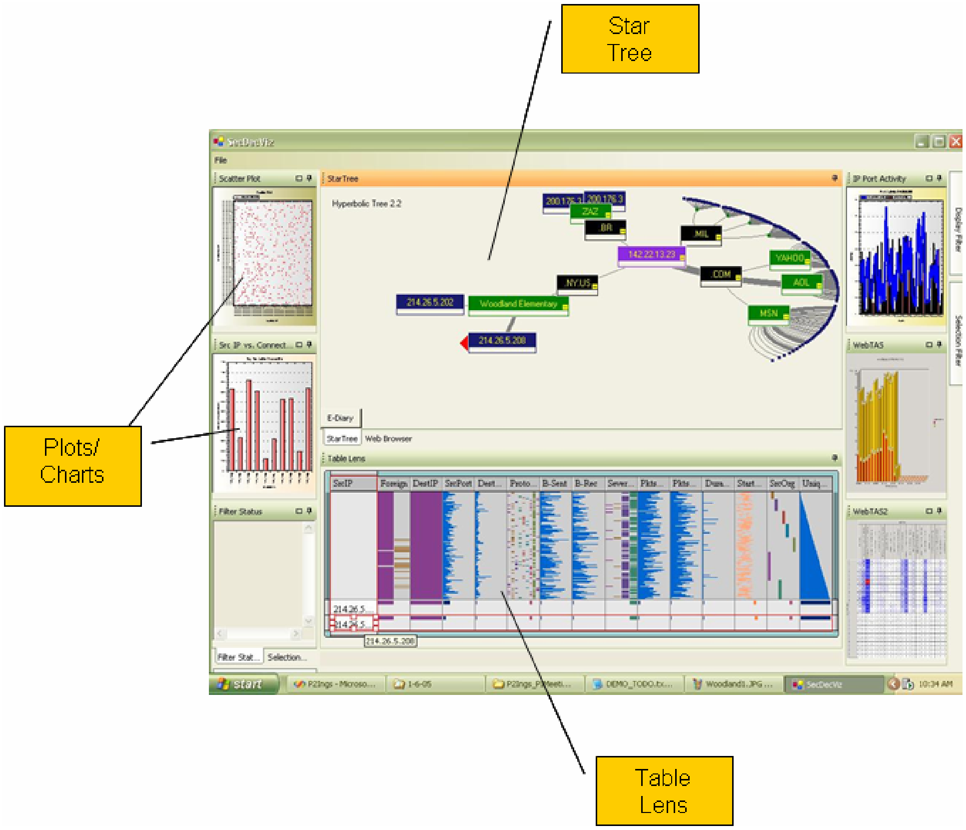

Figure 7. VIAssist Views

In our demonstration, the Star Tree provides a quick look of the number of attackers, their targets, and the mission of the targets. This provides a quick-look indicator that critical systems are under a cyber attack.

The charts and plots are used to convey a number of different information including a series of Top 10 lists. These include the Top 10 Source IPs, Destination IPs, Source/Dest Ports, Countries of Origin, etc.

The Table Lens uses a visual approach to identifying relationships between data. The user selects what data to display and the use of the color bars provides a quick indication of data relationships.

3.5 VisAlert

VisAlert is a tool developed by the University of Utah under funding from DTO. This tool is designed to provide a "circle of awareness" (COA). The COA is illustrated in Figure 9.

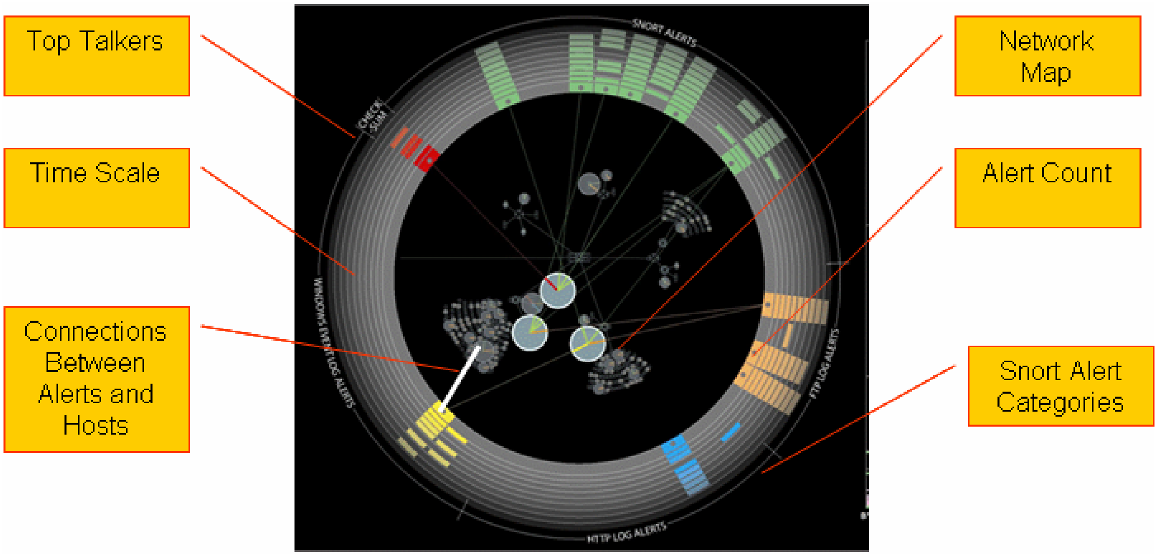

Figure 8. VisAlert Display

The center of the circle represents a map of items of interest. For this experiment, the inner map represents hosts of the network divided into subnets and mission areas. Events appear as colored blocks on the time rings. The number appearing in the color blocks reflects the number of events that occurred. Current activity displays as series of lines that connect the event to the host map in the center of the display. Subsequent bands represent a user-defined period of time in history. The results are that events located on the outer time bands are older than ones that appear along the inner time band. The periphery of the circle is divided into sectors that represent event categories and talkers (e.g., IPs of systems that have generated a number of events).

VisAlert may be operated in historical or near-real time mode. In historical mode, the application queries the IOIN database for all events that occurred during the selected time interval

Interconnecting lines show the activity associated with each of the hosts.

4.0 Scenarios

The demonstration consists of two distinct data sets. The first data captured on the ACC network and second data set consist of lab generated traffic.

4.1 ACC Network Data

Collecting data on the ACC network provides a unique opportunity to analyze real world data. To ensure that some activity would be detected, a constant problem with live data capture, the data collection effort was planned to coincide with a planned network security exercise.

In September 2006, the 92^{nd} Information Warfare Aggressor Squadron (IWAS) was at Langley. During this period, they ran a series of tests as part of a Network Vulnerability Assessment effort. During this period, AFRL had placed two intrusion detection sensors, along with a packet collector, to record the data. The data was stored in the NetD COP/SA database and analyzed using the correlation and visualization tools.

4.2 Lab Generated Traffic

The second set of test data consists of security events triggered on a test network at AFRL. In this data, pre-conceived scenarios are run on a closed network to generate events that the system turns into cyber alerts. The purpose of this data is to show demonstrate how the system responds to various scenarios as the demonstration is given. This also provides an exercising of the full sequence of events from attacker actions to user display.

5.0 Measures of Effectiveness

Measures of Effectiveness (MOE) are needed to demonstrate the success of the effort and serve as a set of metrics for the effort. The MOE's for this effort are as follows:

1. Ability to identify activity from the 92nd data. The 92nd performed several activities while they were onsite. The metric is to determine if the system can detect their activities. The identification of the activity is to occur through correlation (e.g., a cyber alert) and through the visualization tools. The metric will be rated based on the percentage of detections as well as a subjective result of how easily it is to identify.
2. Ability to reduce numbers of alerts. The metric is based upon the ability to provide a reduction in the number of events to cyber alerts.
3. Ability to add mission into awareness paradigm. The metric is to indicate which functions are being attacked and to provide adequate supporting information to analysts and commanders as to the severity of the situation.
4. Ability to display data in a meaningful way, not currently available. This is a subjective rating that will be based upon ACC analyst responses to the system.

A detailed discussion of the metrics from this demonstration will be provided to ACC. The following represents a summary of the results.

5.1 92nd Activity Identification

The 92nd performed a number of different tests. The ASIM and Snort sensors combined, recorded over 3 million events during the test period. These events were analyzed through the visualization tools and correlation engines. The results are as follows:

- FlexViewer provided a spreadsheet style display of all the noted activity identified by the sensors. It also identified suspicious activity from one computer that was not part of the test. The activity was verified after the experiment. Two of the activities, however, would probably have gone unnoticed.
- VIAssist provided a graphical display of all the 92nd activity identified by the sensors. This display also identified the suspicious activity by the computer that was not participating in the experiment. Again two of the activities would probably have gone unnoticed unless the analyst was extremely diligent.
- ECCARS, the Cyber SA engine, identified the majority of the 92nd activity.
- The Sleep Correlator identified all of the noted activity.

5.2 Alert Reduction

During the analysis of the IDS event data it was noted that the Snort sensor was producing a large number of false alarms due to the placement of the sensor in the network topology. Removing these false alarms allowed for the reduction of Snort events from over 3 million to 109,000. The 109,000 events were analyzed by the correlators and resulted in the following reductions.

Sleep Correlator produced 48 correlated events

ECCARs produced 128 tracks (e.g., correlated events)

Both correlators significantly reduced the number of events required for review by an analyst.

5.3 Mission Awareness

The VIAssist display provided a diagram that related high priority signatures and correlated events to the mission of the victim computer. This display provides a quick look into the severity of the attack, computers supporting a mission, and overall mission function.

5.4 Data Display

VIAssist and FlexViewer provide data display capabilities that are not currently available to analysts. We are awaiting feedback from ACC analysts pending a March 2007 demonstration.

6.0 Key Questions

The key questions that are posed by this demonstration are as follows:

1. Do the components either individually or combined provide increased situational awareness ?

2. Are the components intuitive to learn and use?

3. Will the components either singularly or combined make the analysts more efficient or more effective, or require less time or allow more analysis time?

4. What additional features, capabilities, or integration with existing systems are required to further improve capabilities?

5. Do the NetD COP and SA technology components either individually or combined provide a capability that ACC is willing to continue supporting the development and transition of?

6. Are there other IA/CND requirements that these components address, i.e. CAOC, deployed NOSC, IA for Airborne Networking or IA for Wireless Networks?

7. Are there other agencies, services, squadrons, wings, etc. that should see this demonstration?

7.0 Summary

The NetD COP/Situational Awareness effort demonstrates the application of AFRL technology to providing enhanced situational awareness and visualization techniques for network defense. In particular, the program illustrates the following key points:

- Provide an operational view of the network security information
- Move from intrusion detection to attack detection
- Relate the impact of network defense to the larger mission
- Supplement existing/future network defense tools with additional capabilities

The actual software packages used for this effort include VIAssist, VisAlert, Flexviewer, ECCARS, and the SQL correlator.

The results of the effort show that the system is capable of providing an enhanced situational awareness on live network data from a cyber-forensics perspective.

The final demonstration at ACC, originally scheduled for September 2006 is postponed until March 2007 due to scheduling conflicts. As such, this report has been prepared without inputs from ACC. In the interim, we plan on continuing the development of the NetD COP and Situational Awareness systems to enhance the capabilities of network defense personnel.

8.0 Points of Contacts

NetD COP/Situational Awareness:

Brian Spink, AFRL/IFGA, brian.spink@rl.af.mil

VisAlert, VIA Assist:

Walt Tirenin, AFRL/IFGB, wladamir.tirenin@rl.af.mil

ECCARS:

George Tadda, AFRL/IFEA, george.tadda@rl.af.mil